

A note on the least totient of a residue class

M. Z. Garaev

Instituto de Matemáticas

Universidad Nacional Autónoma de México

Campus Morelia, Apartado Postal 61-3 (Xangari)

C.P. 58089, Morelia, Michoacán, México

`garaev@matmor.unam.mx`

Abstract

Let q be a large prime number, a be any integer, ε be a fixed small positive quantity. Friedlander and Shparlinksi [4] have shown that there exists a positive integer $n \ll q^{5/2+\varepsilon}$ such that $\phi(n)$ falls into the residue class $a \pmod{q}$. Here, $\phi(n)$ denotes Euler's function. In the present paper we improve this bound to $n \ll q^{2+\varepsilon}$.

2000 Mathematics Subject Classification: 11L40

1 Introduction

Let q denote a large prime number, a be any integer. Let $N(q, a)$ denote the smallest positive integer n for which $\phi(n) \equiv a \pmod{q}$. The number $N(q, a)$ exists. Indeed, if $a + 1 \equiv 0 \pmod{q}$ then one can take $n = q$. Otherwise, one can take n to be a prime from the arithmetical progression $a + 1 \pmod{q}$.

The problem of upper bound estimates for $N(q, a)$ has been a subject of study of the work of Friedlander and Shparlinksi [4]. In the present paper we obtain a new upper bound for $N(q, a)$.

Throughout, we use the notation $A \lesssim B$ or $B \gtrsim A$ to indicate that $A \ll Bq^\varepsilon$ for any fixed $\varepsilon > 0$, where the implied constant may depend on ε .

Theorem 1. *For any prime q and integer a , we have $N(q, a) \lesssim q^2$.*

Theorem 1 improves the bound $N(q, a) \lesssim q^{5/2}$ of [4].

In the opposite direction, the recent result of Friedlander and Luca [3] implies that there exists a sequence of arithmetical progressions $a_k \pmod{m_k}$ with $m_k \rightarrow \infty$ as $k \rightarrow \infty$ such that $N(m_k, a_k)$ exists and

$$\frac{\log N(m_k, a_k)}{\log m_k} \rightarrow \infty \quad \text{as } k \rightarrow \infty.$$

Following [4], one can look for a solution of the congruence

$$\phi(n) \equiv a \pmod{q} \tag{1}$$

among numbers of the form $n = p_1 p_2 p_3$ with primes p_1, p_2, p_3 . Here one can take p_1, p_2, p_3 to be primes that run certain disjoint intervals $I_1, I_2, I_3 \subset [2, q]$. This converts (1) to the congruence

$$(p_1 - 1)(p_2 - 1)(p_3 - 1) \equiv a \pmod{q}, \quad (p_1, p_2, p_3) \in I_1 \times I_2 \times I_3.$$

If we define I_1 to be the set of primes of the interval $[1, q^{1/2+0.1\varepsilon}]$, then, using Karatsuba's estimate for character sums with shifted primes $p_1 - 1$ and his method of solving multiplicative ternary problems, one can derive that for $\gcd(a, q) = 1$ the number of solutions of this congruence is asymptotically equal to

$$\frac{|I_1||I_2||I_3|}{q-1} + \frac{\theta}{q-1} |I_1| q^{-\delta} q \sqrt{|I_2||I_3|}, \quad |\theta| < 1.$$

From this one obtains the upper bound $N(q, a) \lesssim q^{5/2}$. In the present paper, we aggregate to this consideration one consequence of Huxley's refinement of the Halász-Montgomery method for large values of Dirichlet polynomials. This allows to get the improved upper bound for $N(q, a)$.

Our present application of the theory of large value estimates can be compared with Lemma 4 of Friedlander and Iwaniec [2].

2 Character sums and large value estimates

Let χ be a nonprincipal character modulo a prime q , k be any integer with $\gcd(k, q) = 1$, p be a prime variable, ε be a small positive quantity. When $q^{1/2+\varepsilon} < L < q$, from Karatsuba's estimate it follows that

$$\sum_{L/2 < p \leq L} \chi(p+k) \ll L^{1-\delta}, \quad \delta = \delta(\varepsilon) > 0.$$

To prove our theorem, we will combine this estimate with Huxley's refinement of the Halász-Montgomery method for large value estimates. A sufficient for our purposes form of it is as follows.

Let a_n be numbers with $|a_n| \lesssim 1$, let $0 < V \leq N$ and let R be the number of characters $\chi \pmod{q}$ for which

$$\left| \sum_{n=N+1}^{2N} a_n \chi(n) \right| \geq V.$$

Then Huxley's refinement implies that

$$R \lesssim \frac{N^2}{V^2} + \frac{qN^4}{V^6},$$

see Montgomery [12], Huxley [7], Huxley and Jutila [8], Jutila [10]. This estimate is nontrivial when $V > N^{3/4}$ and $N < q$. In the case $N \geq q$ one has $RV^2 \lesssim N^2$; in the case $V \leq N^{3/4}$ and $N < q$ one has $RV^6 \leq N^3 RV^2 \lesssim qN^4$.

The above sum can be replaced with its ℓ -th moment, where ℓ is a fixed positive integer, and then we have the bound

$$R \lesssim \frac{N^{2\ell}}{V^{2\ell}} + \frac{qN^{4\ell}}{V^{6\ell}}.$$

More generally, the results on large values of Dirichlet polynomials deal with upper bounds for the number of pairs $(\sigma_r + it_r, \chi_r)$, with $\sigma_r \geq 0$ and certain conditions on t_r and characters χ_r (not necessarily distinct), for which

$$\left| \sum_{n=N+1}^{2N} a_n \chi_r(n) n^{-\sigma_r - it_r} \right| \geq V.$$

Such a general consideration is important in applications to zero density problems for $\zeta(s)$ and $L(s, \chi)$. For further key references, see Bourgain [1], Harman [5], Heath-Brown [6], Ivic [9].

3 Proof of Theorem 1

We can assume that a is relatively prime to q , since otherwise the statement is trivial in view of $\phi(q^2) \equiv 0 \pmod{q}$.

Let $0 < \varepsilon < 0.1$ be fixed. Let $k = [1/\varepsilon]$. Put $N = q^{1/(4k-1)}$, $N_1 = q^{1/2+0.1\varepsilon}$.

Let I_1 denote the set of primes $p_1 \in (N_1/2, N_1]$. For $j = 2, 3, \dots, 6k+1$ let I_j denote the set of primes of the interval $(2^{-j}N, 2^{-j+1}N]$. Then, for sufficiently large q ,

$$\frac{N_1}{\log N_1} \ll |I_1| \ll \frac{N_1}{\log N_1}, \quad \frac{N}{\log q} \ll |I_j| \ll \frac{N}{\log q}, \quad 2 \leq j \leq 6k+1.$$

Consider the congruence

$$(p_1 - 1)(p_2 - 1) \dots (p_{6k+1} - 1) \equiv a \pmod{q}, \quad p_j \in I_j, \quad 1 \leq j \leq 6k+1. \quad (2)$$

Note that the left hand side is equal to $\phi(p_1 p_2 \dots p_{6k+1})$ and

$$p_1 p_2 \dots p_{6k+1} \ll q^{6k/(4k-1)+1/2+0.1\varepsilon} \ll q^{2+0.5\varepsilon}.$$

Hence, since $N(q, a)$ exists, it suffices to prove that congruence (2) has a solution for any sufficiently large prime q .

Assume the contrary. We express the number of solutions of congruence (2) (which is equal to zero by the assumption) via character sums. Separating the contribution of the principal character, we deduce

$$|I_1| |I_2| \dots |I_{6k+1}| \leq \sum_{\chi \neq \chi_0} \left| \sum_{p_1 \in I_1} \chi(p_1 - 1) \right| \left| \sum_{p_2 \in I_2} \chi(p_2 - 1) \right| \dots \left| \sum_{p_{6k+1} \in I_{6k+1}} \chi(p_{6k+1} - 1) \right|.$$

The left hand side is $\gtrsim N^{6k} N_1$. Hence, for some $2 \leq j \leq 6k+1$ and $I = I_j$, we have

$$N^{6k} N_1 \lesssim \sum_{\chi \neq \chi_0} \left| \sum_{p \in I} \chi(p - 1) \right|^{6k} \left| \sum_{p_1 \in I_1} \chi(p_1 - 1) \right|.$$

Decomposing into level sets, for some positive numbers V and V_1 we get that

$$N^{6k} N_1 \lesssim R V^{6k} V_1, \quad (3)$$

where R is the number of non-principal characters $\chi \pmod{q}$ for which

$$V \leq \left| \sum_{p \in I} \chi(p - 1) \right| \leq 2V, \quad V_1 \leq \left| \sum_{p_1 \in I_1} \chi(p_1 - 1) \right| \leq 2V_1.$$

By Karatsuba's estimate,

$$V_1 \ll N_1^{1-\delta}, \quad \delta = \delta(\varepsilon) > 0.$$

From the large values estimate,

$$R \lesssim \frac{N^{6k}}{V^{6k}} + \frac{q N^{12k}}{V^{18k}}. \quad (4)$$

Incorporating these estimates in (3), we get that

$$N^{6k} N_1 \lesssim \left(N^{6k} + \frac{q N^{12k}}{V^{12k}} \right) N_1^{1-\delta}.$$

Comparing the orders of the implied expressions, we obtain

$$N^{6k} \lesssim \frac{qN^{12k}}{V^{12k}} N_1^{-\delta}.$$

Therefore, from (4) we get that

$$RV^{18k} \lesssim \left(N^{6k} + \frac{qN^{12k}}{V^{12k}} \right) V^{12k} \lesssim qN^{12k}. \quad (5)$$

Since $N^{4k-1} = q$, the congruence

$$(x_1 - 1) \dots (x_{4k-1} - 1) \equiv (y_1 - 1) \dots (y_{4k-1} - 1) \pmod{q}, \quad x_j, y_j \in I,$$

implies the equality

$$(x_1 - 1) \dots (x_{4k-1} - 1) = (y_1 - 1) \dots (y_{4k-1} - 1), \quad x_j, y_j \in I.$$

This equality has $\lesssim N^{4k-1}$ solutions. Hence,

$$RV^{8k-2} \leq \sum_{\chi} \left| \sum_{p \in I} \chi(p-1) \right|^{8k-2} \lesssim qN^{4k-1}. \quad (6)$$

Let us estimate RV_1^4 . Recall that $N_1^2 > q$ and observe that the number of solutions of the congruence

$$(x_1 - 1)(x_2 - 1) \equiv (x_3 - 1)(x_4 - 1) \pmod{q}, \quad x_j \in I_1,$$

is not greater than twice the number of solutions of the equality

$$(x_1 - 1)(x_2 - 1) = (x_3 - 1)(x_4 - 1) + tq, \quad x_j \in I_1, \quad 0 \leq t \leq N_1^2/q.$$

The right hand side of this equality does not vanish, so for each triple x_3, x_4, t we have $\lesssim 1$ choices for x_1, x_2 . Thus, the above congruence has $\lesssim N_1^4/q$ solutions. Hence,

$$RV_1^4 \leq \sum_{\chi} \left| \sum_{p_1 \in I_1} \chi(p_1 - 1) \right|^4 \lesssim N_1^4. \quad (7)$$

Rewrite (3) in the form

$$N^{24k} N_1^4 \lesssim (RV^{18k})^{3/(5k+1)} (RV^{8k-2})^{15k/(5k+1)} RV_1^4.$$

Taking into account the estimates (5)–(7), we get that

$$N \lesssim q^{(5k+1)/(20k^2+k)}.$$

This contradicts to $N = q^{1/(4k-1)}$.

4 Remark

The reader may note, that in our treating of congruence (2) the only essential property of the sets I_j ($j \geq 2$) that we use is their density in the corresponding intervals, and the set I_1 is used to apply the nontrivial character sum estimate of Karatsuba. Thus, our argument can be applied to deal with a class of other congruences.

Acknowledgement. The author is grateful to S. V. Konyagin for reading the paper.

References

- [1] J. Bourgain, *On the distribution of Dirichlet sums*, II. Number theory for the millennium, I (Urbana, IL, 2000), 87–109, A. K. Peters, Natick, MA, 2002.
- [2] J. B. Friedlander and H. Iwaniec, *The divisor problem for arithmetic progressions*, Acta Arith., **45** (1985), 273–277.
- [3] J. B. Friedlander and F. Luca, *Residue classes having tardy totients*, arXiv: 0709.3056v1 [math.NT] 19 Sep 2007.
- [4] J. B. Friedlander and I. E. Shparlinski, *Least totient in a residue class*, Bull. London Math. Soc., **39** (2007), 425–432.
- [5] G. Harman, ‘Prime-detecting sieves’, London Mathematical Society Monographs Series, 33. Princeton University Press, Princeton, NJ, 2007.
- [6] D. R. Heath-Brown, *A large value estimate for Dirichlet polynomials*, J. London Math. Soc. (2) **20** (1979), 8–18.
- [7] M. N. Huxley, *Large values of Dirichlet polynomials*, III. Acta Arith., **26** (1975), 435–444.
- [8] M. N. Huxley and M. Jutila, *Large values of Dirichlet polynomials*, IV. Acta Arith., **32** (1977) 297–312.
- [9] A. Ivic, ‘The Riemann zeta-function’, Wiley, New York, 1985.
- [10] M. Jutila, *Zero-density estimates for L -functions*, Acta Arith., **32** (1977), 55–62.

- [11] A. A. Karatsuba, *Sums of characters with prime numbers*, Izv. Akad. Nauk. SSSR, Ser. Mat., **34** (1970), 299–321 (in Russian). English translation in: Soviet Math. Dokl., **11** (1970), 135–137.
- [12] H. L. Montgomery, *Mean and large values of Dirichlet polynomials*, Invent. Math., **8** (1969), 334–345.